Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

What is Claimed is:

1. (Previously Presented) A method of providing to a client communications device access to a subscription module of a server communications device, the method comprising the steps of:

establishing a communications link between the client communications device and the server communications device; and

communicating a number of messages (M) comprising data related to the subscription module between the server communications device and the client communications device via the communications link;

wherein the method further comprises the step of providing integrity protection of the messages communicated between the server communications device and the client communications device via the communications link.

2. (Previously Presented) The method according to claim 1, wherein the step of providing integrity protection further comprises calculating, based on a secret session key, a respective message authentication code for each of the communicated messages; and including the calculated message authentication code into the corresponding communicated message.

3. (Previously Presented) The method according to claim 1, wherein the step of establishing a communications link between the client and server communications devices comprises determining a secret session key based on a shared secret between the server and client communications devices.

4. (Previously Presented) The method according to claim 3, wherein the method further comprises providing the shared secret by performing a secure pairing procedure including receiving a passcode by at least one of the client communications device and the server communications device.

5. (Previously Presented) The method according to claim 4, wherein the passcode is at the most 48 bits long.

6. (Previously Presented) The method according to claim 3, wherein the communications link has a secret link key related to it and the method further comprises providing the shared secret by calculating the shared secret using the secret link key as an input.

7. (Currently Amended) The method according to claim 2 ~~anyone of claims 2 through 6~~, wherein the method further comprises:

incorporating a value of a first counter in each of the messages communicated from the client communications device to the server communications device, the first counter being indicative of the number of messages communicated from the client communications device to the server communications device; and

incorporating a value of a second counter in each of the messages communicated from the server communications device to the client communications device, the second counter being indicative of the number of messages communicated from the server communications device to the client communications device; and

wherein the step of calculating a respective message authentication code for each of the communicated messages comprises calculating a message authentication code for each of the communicated messages and the corresponding counter value.

8. (Previously Presented) The method according to claim 1, wherein the method further comprises determining, for the messages communicated from the client

communications device to the server communications device, whether the message is authorized to address the subscription module.

9. (Previously Presented) The method according to claim 8, wherein the method further comprises:

providing a shared secret between the client communications device and the server communications device; and

providing an access control list stored in the server communications device in relation to at least one of the shared secret and the client communications device.

10. (Previously Presented) A communications system, comprising:

a client communications device and a server communications device including a subscription module, the client and server communications devices each comprising respective communications means for establishing a communications link between the client communications device and the server communications device, and for communicating a number of messages comprising data related to the subscription module between the server communications device and the client communications device via the communications link;

wherein the client communications device and the server communications device each comprise respective processing means adapted to provide integrity protection of the messages communicated between the server communications device and the client communications device via the communications link.

11. (Previously Presented) A server communications device including a subscription module, the server communications device comprising communications means for establishing a communications link with a client communications device, and for communicating a number of messages comprising data related to the subscription module between the server communications device and the client communications device via the communications link;

wherein the server communications device comprises processing means adapted to provide integrity protection of the messages communicated between the server communications device and the client communications device via the communications link.

12. (Previously Presented) A client communications device for providing access to a subscription module of a server communications device, the client communications device comprising communications means for establishing a communications link with the server communications device including the subscription module, and for communicating a number of messages comprising data related to the subscription module between the client communications device and the server communications device via the communications link;

wherein the client communications device comprises processing means adapted to provide integrity protection of the messages communicated between the client communications device and the server communications device via the communications link.

13. (Currently Amended) A method of providing to a client communications device access to a subscription module by a server communications device comprising the subscription module, the method comprising the steps of

establishing a communications link between the client communications device and the server communications device;

receiving a number of messages from the client communications device by the server communications device via the communications link, the messages addressing the subscription module; and

wherein the method further comprises the step of determining, for at least one of the received messages, whether the message is ~~authorised~~ authorized to address the subscription module.

14. (Previously Presented) The method according to claim 13, wherein the method further comprises providing integrity protection of the messages communicated between the server communications device and the client communications device via the communications link, where the integrity protection is based on a shared secret between the client communications device and the server communications device; and providing an access control list stored in the server communications device in relation to at least one of the shared secret and the client communications device.

15. (Previously Presented) The method according to claim 14, wherein the access control list is stored in a protected database.

16. (Currently Amended) The method according to claim 14 [[or 15]], wherein the method further comprises calculating, based on a secret session key, a respective message authentication code for each of the communicated messages; and including the calculated message authentication code into the corresponding communicated message.

17. (Previously Presented) The method according to claim 16, wherein the step of establishing a communications link between the client and server communications devices comprises determining the secret session key based on said shared secret between the server and client communications devices.

18. (Previously Presented) The method according to claim 17, wherein the method further comprises providing the shared secret by performing a secure pairing procedure including receiving a passcode by at least one of the client communications device and the server communications device.

19. (Previously Presented) The method according to claim 18, wherein the passcode is at the most 48 bits long.

20. (Previously Presented) The method according to claim 18, wherein the communications link has a secret link key related to it and the method further comprises providing the shared secret by calculating the shared secret using the secret link key as an input.

21. (Previously Presented) The method according to claim 14, wherein the method further comprises:

incorporating a value of a first counter in each of the messages communicated from the client communications device to the server communications device, the first counter being indicative of the number of messages communicated from the client communications device to the server communications device;

incorporating a value of a second counter in each of the messages communicated from the server communications device to the client communications device, the second counter being indicative of the number of messages communicated from the server communications device to the client communications device; and

wherein the step of calculating a respective message authentication code for each of the communicated messages comprises calculating a message authentication code for each of the communicated messages and the corresponding counter value.

22. (Previously Presented) A server communications device including a subscription module, the server communications device comprising communications means for establishing a communications link with a client communications device, and for receiving a number of messages addressing the subscription module from the client communications device via the communications link; and wherein the server communications device comprises processing means for determining, for at least one of the received messages, whether the message is authorized to address the subscription module.